Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies

Katrina Karkazis[1] and Jennifer R. Fishman[2]

Authors:

1. Katrina Karkazis, PhD, MPH
   Senior Research Scholar
   Center for Biomedical Ethics
   Stanford University
   1215 Welch Road, Modular A
   Stanford, CA 94305

2. Jennifer R. Fishman, PhD
   Associate Professor
   Biomedical Ethics Unit, Social Studies of Medicine Department
   McGill University
   3647 Peel Street, 307
   Montreal, Quebec H3A 1X1
   Canada

Short Title (50 character max): Ethics of Biometric Technologies in Professional Sport

Tracking U.S. Professional Athletes: The Ethics of Biometric Technologies

ABSTRACT

Professional sport in the United States has widely adopted biometric technologies, dramatically expanding the monitoring of players' biodata. These technologies have the potential to prevent injuries, improve performance, and extend athletes' careers; they also risk compromising players' privacy and autonomy, the confidentiality of their data, and their careers. Their use in professional sport remains largely unregulated and unexamined. We seek to provide guidance for their adoption by examining five areas of concern: (1) validity and interpretation of data; (2) increased surveillance and threats to privacy; (3) risks to confidentiality and concerns regarding data security; (4) conflicts of interest; and (5) coercion. Our analysis uses professional sport as a case study, however, these concerns extend to other domains where their use is expanding including the consumer sector, collegiate and high school sport, the military, and commercial sectors where monitoring employees is viewed as useful for safety or to maximize labor potential.

INTRODUCTION

Professional sport in the United States (U.S.) is a high-stakes enterprise. With athlete contracts worth tens of millions of dollars and lucrative championships at stake, professional sport has long strived to optimize the physical performance of its employed athletes, who must perform under conditions of stress, including fatigue, overexertion, overtraining, and sleep deprivation. Each of these increases the risk of injury and soft tissue damage—principal threats to playoff chances. These conditions are not just unfortunate; they are incredibly costly. Some have calculated that the National Basketball Association (NBA) lost $2.7 billion due to injury over nine seasons, with some teams losing as much as $50 million per season (Stotts 2014; Talukder et al. 2016).[1]

With so much at stake, professional teams have become laboratories devoted to preventing injury and enhancing performance (King and Robeson 2007; King and Robeson 2013). Among these measures is the increasing use of biometric technologies to monitor players, technologies that one sport scientist we spoke to characterized as "critical for asset management." All major professional sports leagues in the U.S. are using these technologies, including the National Football League (NFL), Major League Baseball (MLB), the National Hockey League (NHL), Major League Soccer (MLS) and the NBA.[2]

Teams have long assessed and monitored their athletes' physical condition. These technologies represent a departure from previous monitoring methods in both breadth and depth. No longer limited to self-reporting and metrics like vertical jump, new wearable biometric technologies offer the potential to monitor athletes' physiology around the clock, on and off the field, and teams are heavily and readily investing in this surveillance. The devices include, for example, heart rate and sleep monitors, electrocardiogram (ECG) and electroencephalogram (EEG), with data being transmitted to laptops, tablets, and mobile phones and stored on companies' and teams' central servers. Because of the convenience with which they are obtained, the biodata are more varied and extensive than ever.

Professional sports teams use biometric technologies for purposes that range from managing training to preventing injury. Some apply the technologies as motivational tools, believing that they offer objective feedback to players to modify behavior, deter complacency, or detect laziness. Teams are also exploring the potential of these technologies for longer-term applications, such as assessing the career longevity of current players and potential draft picks.

The popular conversation around these technologies thus far is overwhelmingly enthusiastic, emphasizing their potential to predict and prevent injuries and enhance athletic performance. If applied judiciously, responsibly, and ethically, biometric data technologies in professional sport have the potential to reduce injuries, improve performance, and extend athletes' careers. However, these same biometric data come with the risk of compromising players' privacy and autonomy as well as the

confidentiality of their data. Moreover, they also have the potential to disadvantage players in contract negotiations and to harm, and even cut short, athletic careers.

Whereas in U.S. health care settings and biomedical research, biometric data is governed by regulations on informed consent, the Health Insurance Portability and Accountability Act (HIPAA), and other data privacy assurances, their use in both the professional sport and consumer sectors remains largely unregulated and unexamined. Furthermore, the collection and storage of biometric data by employers and third parties raises risks of exploitation, coercion, and employee discrimination when these data are used in hiring and firing decisionmaking.

We seek to start a deeper discussion of the adoption of these technologies by examining five areas of ethical concern: (1) data validity and interpretation; (2) increased surveillance and threats to privacy; (3) risks to confidentiality and concerns regarding data security; (4) conflicts of interest; and (5) coercion.

Our analysis draws on reviews of the literature as well as on select empirical data, including interviews with those who develop and utilize these technologies within professional sports teams as well as the authors' attendance at conferences where they have been discussed (Stanford IRB approval 32613).

Although our analysis uses U.S. professional sport as a case study, the purposes and contexts in which these technologies are used raise similar ethical concerns for both collegiate sport, where these technologies are widely in use, and high school sport, where their use is growing. They further extend to the military where they are used to inform soldier planning and task delegation based on an individuals' physiological responses under stressful conditions, as well as commercial sectors where monitoring employees is viewed as useful for safety or to maximize labor potential (Hoyt and Friedl 2016; Mehlman 2015; Mehlman and Li 2014; Silverman 2016). As these technologies become more mainstream, less expensive, and more broadly marketed, the push to use them in more mundane work and school

environments in order to incentivize “fitness,” save health care dollars, monitor productivity, and surveil student/employee safety will increase (Silverman 2016). Our discussion is also relevant to the rapidly expanding technological development and use of consumer wearables, which have not been matched by an equivalent evolution of data or privacy governance models which could attend to the privacy implications of having an extraordinary amount of data points that could be collected, aggregated across devices and analyzed. We begin the discussion with biometrics in professional sport in order to highlight the unattended ethical issues arising in places where these technologies are already being put to use and elsewhere as technology is diffused to other areas.

BIOMETRIC TECHNOLOGIES AND APPLICATION IN SPORT

Biometrics is the measurement and statistical analysis of physical and physiological characteristics. The term frequently refers to identification and authentication technologies. We use it here in the manner of those in sport to refer to the measurement and tracking of physical and physiological characteristics for the purpose of assessing performance and recovery.

Many of these technologies are packaged into wearable devices that upload data (via Bluetooth or another wireless technology) for storage and analysis in the cloud or on a computer, tablet, or mobile phone. Some systems rely on wearable GPS trackers that monitor real-time accelerations, decelerations, changes of direction and jumping (measuring both height and frequency) during play (e.g., Catapult Sports®). Calling itself the “Google Analytics for sports,” Catapult Sports claims to assess athlete “risk,” “readiness,” and “return to play.” It counts at least half of the NBA and NFL teams as clients (Westover 2016).

Other systems track physiological markers and behaviors in different formats. The Zephyr Bioharness™, for example, is worn around the torso and tracks heart rate and heart-rate variability (HRV), breathing rate, and movement. WHOOP®, a wristband device, tracks similar biovariables and is

marketed as a “performance optimization system” that gives scores for strain, recovery, and “sleep performance,” as well as to predict performance (“WHOOP” 2016). Some devices use adhesive bandage-like patches with sensors (e.g., WiSP™) that continuously measure variables such as heart rate, respiration, motion, blood oxygenation, brain activity, muscle function, body temperature, changes in blood pressure; some track a “whole library” of chemicals present in sweat including electrolytes, proteins, and heavy metals (Gao et al. 2016). Inventors imagine “a pathology lab on your hand” (as quoted in Swetlitz 2016). The most important innovative aspect of these technologies is their noninvasive, portable biomonitoring capacity to continuously collect data for days.

Although some devices are specifically developed for sport, others are adapted from medical technologies. The Omegawave™, for example, aims to assess what it calls “readiness,” using vital signs obtained through a one-lead ECG and EEG (to track and record brain wave patterns). The system is portable though not wearable. Data collected are uploaded to the company’s website for analysis and made available to a coach or trainer.[3] The analysis provides assessments of the athlete’s cardiac health, metabolism, central nervous system, gas exchange, detoxification status, and hormonal system. Billed as “your personal health lab,” Kenzen makes a “smart patch” that syncs with a mobile phone and is “quietly measuring around the clock” variables like vital signs, motion, fluid and nutrients (http://www.kenzen.com/). Developed for sport, it aims to move into the clinic and to consumers directly.

Those working with teams and the technologies envision a broader scope of tracking via implantable and ingestible technologies that would enable what has been called “überveillance,” omnipresent surveillance using biodata, movement, and location tracked by technologies embedded in bodies (Michael and Michael 2007). Currently used to monitor prescription medication adherence, these technologies are being adapted for sport with the aim of offering more precise and continuous monitoring of athletes’ bodily or biological processes and reducing athlete hindrance and device damage

during use. One NBA lawyer foresees the adoption of these and more, “It’s going to be ingestibles; it’s going to be implants; it’s going to be everything, tracking not only sleep movement, not only how fast you’re running. It’s going to track how your body is digesting certain supplements; it’s going to be tracking maybe even genes… the Catapult stuff, that’s like maybe 5% of what is actually going to be tracked.”

REGULATION OF BIOMETRIC TECHNOLOGIES

At present, there are few regulations governing the use of biometric devices in professional sport. Professional athletes are considered employees and thus are protected by federal and state employment regulations. Legal restrictions on employers' access to medical information as outlined in the Americans with Disabilities Act (ADA) and the Genetic Information Nondiscrimination Act (GINA) should theoretically apply to team sports. The ADA mainly applies to health exams before hiring and it, along with GINA, have “health and safety” loopholes that could allow for much of the current biometric technology use by teams. Thus protection from federal regulations like GINA or the ADA are, at best, uncertain and more likely insufficient.[4]

Even though athletes are protected by federal and state employment regulations, by signing player contracts they agree to be governed and abide by collective bargaining agreements (CBAs), the basic employment contracts between team owners and the players’ unions. As long as the CBAs do not violate or infringe upon federal laws or human rights, and no actions are brought claiming such, they will continue to dictate the boundaries of team-player relationships. Currently, however, the CBAs of the professional leagues largely do not address biometric technologies’ uses, and the rare agreements that do, do not address issues of data governance (the overall management of the availability, usability, integrity, and security of the data). The NBA’s CBA, for example, makes no mention of the collection of biometric data or wearable devices, but a 2014 memorandum (Ligaya 2014) sent to teams notes the

possible competitive advantage offered by such devices and states that these devices may be worn only during training and practice, not during games (likely because their use had not been agreed upon in the prior CBA and out of concern about them compromising player's ability to play). They are permitted during games in the NBA's D-league, "the league's research and development laboratory," and used for hiring decisions (http://dleague.nba.com/about/).

The current MLB CBA, which expires near the end of 2016, makes no mention of the biometric technologies, but the Associated Press reported that the MLB will allow two devices, one of which is the Zephyr bioharness, for in-game use starting in the 2016-17 season (Associated Press 2016b). Under the recently renegotiated CBA of the NHL, players are not allowed to wear these devices during games. The most recent NFL CBA from 2011 (which runs through the 2020 season) says players may be required to wear "equipment that contains sensors or other non-obtrusive tracking devices for purposes of collecting information regarding the performance of NFL games, including players' performances and movements, as well as medical and other player safety-related data" during games and practices (NFL 2011). In late 2015, the NFL Players' Association (NFLPA) filed a grievance against the league and its 32 clubs over the use of sleep monitoring devices during off-time and requested member clubs immediately cease and desist from using the devices unless approved by the NFLPA (Perez 2016).

Although the MLS CBA does not refer to the use of these technologies, Fédération Internationale de Football Association (FIFA), the international governing body of soccer, does not allow the use of transmitting devices in official league games. Teams have, however, been wearing such devices in the reserve league.

Biometric technologies are currently part of some leagues' CBA negotiations. Players may be willing to accept their mandated use as a bargaining point in return for things like higher salary caps, especially with their promise of improved performance and reduced injury. In so doing, they, and those

concerned with the best interest of players, should understand what they would be accepting: the technologies' risks as well as their benefits.

ETHICAL ISSUES IN THE COLLECTION AND USE OF BIOMETRIC DATA

There is a growing literature on ethical issues in the use of biometric data for personal use (e.g., Schüll 2016) and in healthcare (Greene 2016; Lupton 2013). Here we focus on the particular ethical concerns that arise with the implementation of these technologies for optimizing the performance of professional athletes. Integral to these concerns is that parties other than the individual athlete are also interested in and invested in these data: coaches, team owners, team trainers, agents, and leagues as well as third parties such as fantasy sports enthusiasts. These stakeholders' access to and possible use of biometric data give rise to particular ethical concerns including: (1) validity and interpretation of data; (2) increased surveillance and threats to privacy; (3) risks to confidentiality and concerns regarding data security; (4) conflicts of interest; and (5) coercion.

Validity and Interpretation of Data

The appeal of biometric technologies in sport rests heavily on the perception that they are more precise and objective than other measures and metrics of complex conditions (such as athlete fatigue), that they operate without or with less error or bias (are more accurate) than these other methods, and that they yield data that are easily interpretable and actionable. One company CEO, for example, asserts, "We can analyze the status of the human body in just two minutes, looking at all the different factors that contribute to performance" (as quoted in Pappas 2014). The assumption that biometric data reduce error, bias, and uncertainty over other methods carries with it the risks of over-determination of the results and of subsequent harms to some players, including pushing them too hard or, conversely, wrongly assuming that they are fatigued or are unfit to compete (temporarily or ever).

In examining the ethical issues raised by the use of such technologies, an initial and central

question is whether they deliver on their claims. Are the data being collected reliable indicators of the characteristics they purport to assess (or at least more reliable than previously used, less invasive, and less risky methods)? Do the technologies (when used correctly and as directed) collect accurate data? Are the technologies being correctly used? There are also questions of interpretation: Are the companies' proprietary algorithms able to operationalize the complex concepts they hope to quantify? Do those collecting and using the data at the team level know how to analyze and interpret them, and are they aware of their limitations?

Without suggesting that technology needs to be perfect in order to be put into use, we nevertheless believe they should be reliably better than other currently available methods given their potential for exposing players to greater risks. There is currently no standard for evaluating the technology nor leagues' and teams' adoption of new methods. As such, there is no way to know whether and to what extent they improve upon previous practices, or the risks associated with their adoption.

Using heart rate variability (HRV) as an example, we highlight ways in which these factors come to matter for biometric technologies. HRV, a measure of the changes in the time elapsed between heart beats, has long been used to assess risk for patients with cardiac disease. In recent years, HRV monitoring has become popular in professional and even recreational sports to assess overtraining owing to the development of affordable and easy to operate smartphone apps and other technologies. Generally, the higher the HRV, the better. Lower HRV is understood to indicate fatigue and stress. Thus, if an athlete's HRV decreases, trainers might reduce the intensity of workouts or restrict play.

Because it is a relatively new method for assessing overtraining in sport, we need to ask whether HRV measurement is a useful tool to assess athlete recovery or improve performance. There are at least two components to measuring HRV: the technology itself and its operator. Then there is a

two-fold question as to the data collected: is it accurately measuring HRV? And is HRV being adequately interpreted? Measuring cardiac activity with a wearable sensor, mobile technology, or other commercially-developed technology may seem like a straightforward scientific and value-neutral technique, but it is quite complex. In clinical contexts, HRV is measured by electrocardiogram (ECG), a device that is widely considered to extract reliable and valid data.

Can wearable technologies "accurately" measure HRV? The answer depends on the technology and the operator. As one example, some apps claim to measure HRV by placing one's finger over the LED flash and camera to track changes in arterial pressure (known as photoplethysmography). The camera quality, the proximity of the illuminating LED to the camera lens, and the technology's capacity for data processing all impact measurement accuracy. As one observer said, "Because these trackers are so new, and because there's no consumers' lab checking them against, say, clinical-grade equipment, we have no idea about their accuracy" (as quoted in Ghose 2015). Most of the consumer devices on the market have very little or else poor quality science behind them and are not, for example, medical devices approved by the FDA. To what degree have they been tested or validated? Not only may they suffer from inaccuracy, but they cannot take into account individual variability, a point to which we return.

Accuracy is also heavily dependent on the operator. HRV measurement is very sensitive to movement: the more movement, the more "noise" in the data. HRV measurement also requires attention to body position and time of day: like basal body temperature, HRV is best measured immediately after awakening and before any physical activity has been undertaken. There is no consensus, however, on the length of time for which the heart rate should be measured. The factors involved in achieving a reliable and valid HRV measurement are manifold and subject to operator error and use variability.

Even if the data accurately track HRV, can HRV be interpreted as indicating fatigue, injury

vulnerability, and so on? HRV interpretation is complex, leading to considerable confusion for many regarding how the measurement is meaningful for athletes. HRV varies greatly between individuals and is individually dynamic, varying by age, day and even hour, as well as body position. There is also interindividual variation in HRV responses to training in team sports (Nakamura et al. 2016). This complexity may make it difficult to know what is "normal" for an individual. For sport, HRV seems to be most reliable and useful when athletes are frequently monitored to assess trends in an individual's HRV. Teams, however, often have spotty HRV data owing to athlete monitoring overload, noncompliance, and travel schedules. With so few data points, knowing what one particular value means becomes much more difficult. Although the ability for at-home measurement may theoretically help to increase the number of data points, this is only useful if these technologies are used correctly by athletes, and if they provide reliable readings.

This is only the beginning of the issues with HRV interpretation. It is a common belief that high HRV is good and that low HRV is an accurate marker of the acute training fatigue that can compromise player performance. But this isn't always so.[5] HRV change can occur for many reasons, including stress or excitement, and thus may not have any connection to "readiness." If an athlete's HRV is low, there is no way of knowing whether that reading is due to overtraining or because of traffic on the drive to the training facility. Some research shows pre-competition anxiety and anticipation can decrease HRV (Edmonds, Sinclair, and Leicht 2013; Morales et al. 2013). In short, context matters: even with accurate readings, the interpretation of those readings remains a challenge.

Companies aim to break through this complexity by simplifying things for the non-expert user with green-light/red-light type signals. These assessments are sometimes based on HRV alone, but quite often HRV assessment is part of a company's proprietary algorithms combining multiple physiological factors. While algorithms may seem "objective," they always reflect assumptions, perspectives, and biases. Companies are not required to vet their algorithms, nor are they held accountable for their

validity (Angwin 2016). When thinking about the utility of an algorithm, it is not simply a question of whether it is the right algorithm for the job, but whether a concept like athlete recovery can ever be captured by an algorithm.

To ascribe significance to an athlete's biometric data, the values must be compared to an existing data set. Currently, guidelines for interpreting HRV fluctuations are based on a dataset from the general population and may not be applicable to athletes, whose cardiac capacity and HRV are much higher than average. According to Euan Ashley, a Stanford professor of medicine and genetics, "I'm not sure you really get anything useful from it that anyone can really interpret in a clear way…I would say we don't yet have the training set for athletes."

In addition to not having an appropriate referent population, it is questionable whether current algorithms to interpret biometric data are sophisticated enough to yield useful predictions. Although ECG can provide data about blood flow as an indicator of heart function, the question of how these data, when combined with the EEG (which provides very little information about important qualities such as fatigue, overtraining, or performance levels), can produce a reliable metric like "athlete readiness," still remains. These algorithms are proprietary and therefore kept secret; those relying on them outside the company are given no information about their compilation. Rather, they must rely on outputted dashboard readings. At present, sports biometric analysis faces the paradoxical problem of being overloaded with data that require interpretation while being bereft of the historical data needed to create valid algorithms. In short, the signal-to-noise ratio in biometric data remains low, particularly for athlete populations.

Another common use of biometric technologies in sport is assessing load, recovery, and the severity of injury. Historically these assessments have depended on self-reporting of pain and exertion—inherently subjective measures, and ones that athletes may consciously manipulate in order to maintain playtime, standing on the team, or to appear stoic, among other reasons. Biometric devices hold the

promise of more “objective” measures. For example, some sensors can detect mechanical inefficiencies in the knee. These can be measured over time to assess improvement or deterioration after injury. But when we asked a company representative whether the sensor technology could prevent injury, he hesitated: “The huge issue is how spotty the data can be and also what to make of it. Too often, we don’t know.” Nevertheless, the Seattle Sounders said the implementation of these technologies led to a 67% reduction in game days lost due to muscle injury from 2012 to 2014 (Tenney 2015).

The increase in prevalence of seemingly “objective” measures raises other concerns especially if they are not interpreted properly. One sport scientist relayed how misuse of biometric data led to two athletes sustaining season-ending injuries in the pre-season after a professional sports team had just adopted the technology for use in practice. The scientist and a company representative had trained the strength coach and assistant strength coach in its use. At the start of the pre-season, the head athletic trainer who had not been trained to use the technology, took charge of its implementation. This included assessing a quantitative "load score," which is an indicator of overall athlete "work." Players in the sport have different loads, based on both their individual movement efficiency, and the movement demands of their position. The head trainer decided to assess and "average" player load from athletes involved in high intensity efforts that he felt would be a good benchmark for the entire team. When any player reached 85% of that load, the trainer removed that player from practice. Because of individual variability, players amass loads at very different rates. Those amassing loads faster were taken out of practice regardless of whether they felt fatigued. Those who amassed loads more slowly were kept in practice. The players who were kept in practice longest were under much more physical stress than those who were taken out, in part because they also now had to assume the workloads of the removed players’ positions. Eventually, the last two players remaining in the position sustained significant hamstring injuries—despite using technologies that were supposed to protect them from injury. The trainer failed to understand that athletes’ initial load baselines differ, that group averages cannot be

applied to individual athletes, and that one cannot use linear quantification and regression analyses to prevent injury in a complex human system.

Additionally, the use of biometric technologies also runs the risk of reifying the idea that the body can reveal a truth about someone in place of or despite their subjective claims or an individual's own assessment of their well-being and subjective bodily experience. Many athletes have high pain tolerance, for example. Moreover, there are many variables that affect an individual's pain tolerance. It is not clear that these devices are better able to measure severity of injury than metrics for pain that are self-reported. But once these technologies become part of the infrastructure of team training, their reliability may be taken for granted and therefore never appropriately evaluated. This is a common and well-known process as new medical and bodily technologies become integrated into practice and routinized (Braun 2014; Joyce 2008; Rapp 1999; Timmermans 2010; Dumit 2004). As King and Robeson note, in the context of major league sports, "the pervasive atmosphere of progress, innovation, and data gathering make athletes surprisingly like patients-subjects in a clinical research environment" (2007, 2013).

Surveillance and Privacy

Because teams have a strong interest in gaining comprehensive information about players' health and performance, sport already pushes the limits of the employee-employer relationship with respect to privacy and surveillance. Professional teams have nearly unrestricted access to health information, not just for players under contract but for prospective players. At the NFL scouting combine, for example, every college football player is evaluated by at least one doctor who might assess "cardiovascular, kidney, liver and pulmonary health," by administering "a battery of tests—such as blood work, EKGs and, for certain players, stress tests for their heart" (Siebert 2014). These data are then shared among teams.

This open access creates expectations for signed players to submit to medical exams and surveillance (as outlined in the leagues' CBAs and players' contracts). As McChrystal notes, "Each of the standard player contracts contains some form of language stating that the player agrees that he will remain in top physical condition and is physically able to perform up to the best of his abilities" (2014, p. 168). The phrase "best of his abilities" is subjective and the extent to which biometric data are used to determine whether a player is satisfying this vague requirement is unregulated.

Wearable biometric devices not only track important biodata, they offer the potential to monitor athletes' locations, movements, and behaviors around the clock, on and off the field. Even before the advent of mobile health devices, teams sought to monitor off-the-field behavior. As one coach offered, "There is a lot of unmonitored time where they're making bad decisions." The typical approach to monitoring has been to require athletes to fill out self-report questionnaires and submit to occasional drug testing. Evidence that an athlete has violated team rules (for instance, drinking heavily the night before a game) may be grounds for terminating his contract or at least suspending him from play. Now, however, a wearable device that tracks sleep and includes GPS may reveal how late a player was out, whether he was drinking or speeding, or whether he had sex. As one NFL trainer said, "This information definitely goes to the coaches because that athlete is not going to recover, so they're an injury risk."

Teams may say that their interest is not to spy on their players: one trainer maintained that the goal of using biometric data is for the players' own benefit, "to make them healthier and maximize their careers." Nevertheless, team officials' access to these data and information creates anxieties among players. "The players, a lot of them hate it. They think we're using it for something that we don't have any intention to," said another trainer. While some player suspicion may be unwarranted, trainers and coaches nevertheless sometimes have a conflict of interest between their players and the organization that employs them. Often, these data inform decisions that are both beneficial to a player and a team's

long-term goals (protecting its investments by increasing overall player productivity and career longevity). However, at times, trainers and coaches may use data to make decisions that ultimately run counter to a player's wishes, and perhaps involve disclosing private player information to team management.

Confidentiality and Disclosure

Surveillance and privacy are primarily issues of autonomy. They relate to what is tracked, when it is tracked, how it is tracked, and what the tracking reveals (heart rate, temperature). Confidentiality is an extension of privacy in that it applies to the data already collected and access to those data: who sees them and how they are protected and used (or misused). Increased surveillance, both at and outside work, and technologies that provide information on physiological attributes and behaviors, give teams nearly unrestricted access to players' personal data. Because this information is also of considerable interest to leagues, other teams, fans, and various other stakeholders in professional sports, its collection raises unprecedented concerns about confidentiality and data security. Who is granted access to players' biometric data and for what purposes? And who grants such access? Do athletes have any control over the dissemination of their personal data, especially to third parties? Of particular concern is whether the player has any say or financial benefit if the league or team sells their data either in identifiable, de-identified or aggregate form. If athletes agree to some types of biometric monitoring as a condition of their contracts, have they implicitly agreed to increased surveillance as the capacity of the device in question expands?[6] Have they consented to the sharing of all of the collected data? And are there protections in place to prevent unauthorized sources from accessing these data?

Although some team personnel, such as doctors, may be bound by professional standards of confidentiality, others, such as trainers, physical therapists, and coaches, are not. What's more, staff may view the data as performance data rather than confidential medical or health information and disclosure of biometric data may be viewed differently based on whether it is understood as health

information, performance information, or behavioral information. In some contexts, confidentiality issues can be addressed by anonymizing personal data. For teams, however, the value and utility of biometric data mostly depends on its being linked to individual players.

League Data Sharing Policies

The most glaring omissions regarding data confidentiality are in the agreements that govern the sharing of data with third parties such as other teams, the public, and even carriers of health or life insurance. Although players have strong incentives to avoid public disclosure of health information, collective bargaining has resulted in greater disclosure to teams as players "bargain away most of the privacy protection" (McChrystal 2014). The increasing amount of personal and health information available to teams from players' biometric devices, however, renders these issues more pressing.

League documents such as CBAs and health information authorizations (HIAs) cover a team's authority to disclose a player's medical information to other parties. All of the leagues provide for some degree of public disclosure of player medical information, mostly as it relates to injuries and their treatment. In addition, some leagues have players sign virtually unrestricted HIAs that allow teams to share health information more broadly. NBA players, for example, sign a blanket HIA at the beginning of each season. Although this is theoretically voluntary, one team lawyer noted that he had never heard of a player not signing it. The HIA allows a player's team to disclose any medical or other information that could affect a player's ability to play "skilled basketball" to physicians, other teams, D-league teams, and "basically anybody that's NBA-related." If a player is traded, the team has the authority to send that player's health records to the acquiring team. If the NBA asks a team for information on a player's medical condition, the team does not have to ask the player before sharing this information.

The MLB's HIA defines "health information" as "my entire health or medical record, including, but not limited to, all information relating to any injury, sickness, disease, mental health condition,

physical condition, medical history, medical or clinical status, diagnosis, treatment or prognosis, including without limitation clinical notes, test results, laboratory reports, x-rays and diagnostic imaging results" (King and Robeson 2013; Major League Baseball 2005). As one team lawyer said, "I have to think about best practices and protecting our athletes' data. The good thing is that . . . the athletes sign a pretty broad waiver that essentially waives their right to have the privacy that a normal person would expect, so we don't have that to worry about." While waivers might legally protect teams (although they have yet to be tested in court), they are not concerned with the broader ethical issues at stake in the distribution of players' biodata.

Not only do NBA D-League players agree to undergo any medical exams requested by any physician, but contracts and HIAs also further stipulate that "any Health Information disclosed may be redisclosed by the recipient of such information, that I will sign any additional individual authorizations as may be requested by NBADL or Team to facilitate disclosure of Health Information, and that NBADL shall not be obligated to me for any medical expenses or damages"(NBA D-League 2015). The contract refers to "redisclosure," a seemingly intentionally imprecise term that *de facto* allows the sharing of information with anyone they choose.[7]

With so little protection of personal data from third-party disclosure, critical questions arise regarding who might gain access to these data. For example, wearable device companies that collect data can be subpoenaed. Moreover, these companies' privacy policies often say that they will release data in response to legal requests. Fitbit®, for example, says it will release data "necessary to comply with a law, regulation, or valid legal process" ("Fitbit Privacy Policy" 2016). Fitbit has released data for legal cases where the activity of the plaintiff or defendant is admissible as evidence (e.g., Gershman 2016).

When disclosed, biometric data could cost professional athletes millions of dollars and even end careers as information revealed by these devices could be interpreted to allege that a player violated

team conduct rules or is a liability in some way. Michele Roberts, executive director of the players' union, said that her "greatest concern is how some of this information might be leaked or used in contract negotiations" (as quoted in Lowe 2015). In addition, disclosures could affect endorsements and other income opportunities, both during the athlete's career and thereafter. Then there are health insurers who might seek this information to charge more or deny coverage based on such factors or in a player's future. Would these data be admissible in criminal proceedings such as allegations of assault or drunk driving?

Federal and State Health Privacy Laws

Although the privacy of health information is protected by federal and state laws, the applicability of these laws to athletes' biometric data is unclear. HIPAA provides individuals with important privacy rights and protections over their health information, including restrictions on how this information is used and disclosed by health plans and health care providers. HIPAA is applicable to most health care providers (known as "covered entities"); however, a recent report by the U. S. Department of Health and Human Services (HHS) noted that new and emerging health technologies are not covered by HIPAA (U.S. Department of Health and Human Services 2016). The report outlines the significant gaps in privacy and data security protections, and thus consumer protection, that can make information vulnerable. Moreover, it does not recommend expanding HIPAA to address these contexts. Specifically, the HHS has said that "Professional sports teams are unlikely to be covered entities" (U.S. Department of Health and Human Services 2002). HHS reasoned that an athlete's medical records may be deemed to be part of their employment records rather than privileged health information, thus allowing sharing within, but not outside, the employing organization (Malcolm 2016): "Even if a sports team were to be a covered entity, employment records of a covered entity are not covered by this Rule…nothing in this Rule prevents an employer, such as a professional sports team, from making an employee's agreement

to disclose health records a condition of employment" (U.S. Department of Health and Human Services 2002). The implications, had the law been applicable, would have been huge, requiring teams to hire a compliance officer and institute new practices including ones preventing the disclosure of medical information to reporters. Players have an interest in protecting this information because it can affect their position when negotiating contracts. Even if medical privacy laws covered these data, HIPAA makes exceptions for queries from law enforcement and national security agencies, as well as many other legal requests.

As McChrystal notes, "The operating principle suggested by HHS is that a player may be compelled to authorize the release of medical information to his team without violating federal health care privacy regulations under HIPAA. Therefore, players can be compelled to consent to disclosure of information about their medical condition without violating privacy principles under federal law. The same is generally true under state law" (2014, p. 166). Even if sports teams were covered entities, legal protection for medical privacy is waived when the individual consents to disclosure, as every player does through the CBA, the uniform player contract, and HIA.

As users of commercially manufactured biometric devices, athletes may also be providing information to a database maintained by the manufacturer. Although we have not seen the contracts the companies provide to team management, many companies' privacy policies are vague. Because these data are not viewed as protected health information (PHI) under HIPAA, and because of the broadly-worded HIAs athletes sign, it seems that manufacturers can legally share players' sensitive medical data. Some teams use technologies from multiple vendors and share data among vendors. One company that makes a sleep tracking device acknowledges HIPAA (http://lark.com/hipaa-privacy-policy/); however, this appears to be the exception rather than the norm (Lark contracts with health insurance companies, requiring the company to comply with HIPAA).

Some states have privacy rules stronger than those in HIPAA that require court agency for disclosure of medical information. In California, for example, search warrants for medical records require judicial approval based on probable cause. California also allows disclosures of health information with no consent in response to certain legal requests. Whether state laws protect players from this kind of disclosure will, in part, depend on where the data are held and where the player lives. Multiple state level authority could be at issue if player residence, team and technology corporate residence, data storage and other locations are taken into consideration.

Organizations should also consider whether mandating wearable technology to monitor their employees' performance, health and well-being may also give rise to other legal risks or issues under workplace health and safety laws. For example, if the information collected from these technologies means that an employer knows, or could reasonably know, that an employee has not had much sleep in recent days or was stressed or injured, does that employer have a duty to the employee, other employees, or the organizations for whom the member is undertaking work under a contract, to ensure the employee doesn't participate in an activity that could be affected by their lack of sleep, state of mind, health, etc.? Would the employer be liable if the employee injures themselves or a member of the public, or other team member?

Data Access, Storage, and Security

Within a team organization, biometric data from individual players could be viewed and used by athletes, agents, general managers, trainers, coaches, and owners. Policies on data access and security show little consistency across teams, however. Some teams limit employees' access to particular types of data, or provide athletes with devices for monitoring data that are not shared with coaches. For example, players might be issued sleep-tracking devices whose data are not uploaded for use by coaches. In some organizations, only the trainer has direct access to the data, whereas in others the

owners may also see the data and use them as a basis for team selection. Jeremy Holsopple, athletic performance director for the Dallas Mavericks, says he tells athletes “that nobody sees the data but me and the people directly on staff that work for me” (as quoted in Torre and Haberstroh 2014). The coaching staff, however, “will get what they need to make decisions as coaches. But we will not give them the things that players can be judged upon” (as quoted in Torre and Haberstroh 2014). How the need for access is determined is far from clear, and neither are the limits and rationale for data accessibility. How does a team know how or where to draw the line on these questions?

In addition to deciding who should have access to players’ personal data, teams and technology companies are obligated to secure data against unauthorized access and unauthorized use. In clinical settings, safeguarding and encryption of electronic health information are subject to rules and best practices. From what we know, teams and companies are using much less rigorous data-protection measures than hospitals or large cloud-based companies. This is troubling considering the US. healthcare industry historically has had the highest rate of security breaches of any industry, accounting for 25% of all known breaches (Huq 2015; McCarthy 2015). Some studies estimate that as many as 90% of healthcare organizations have had a breach of security over the prior two years (Ponemon Institute 2016; Korolov 2016).

All mobile health technologies produce data outside of these protected settings and may be vulnerable to security breaches. Personal data from professional athletes, who are the subjects of considerable media attention, may be at particularly high risk of hacking. At a recent panel on data ownership at SXSW Conference, one of the authors asked the panelists about best practices around data security, to which there was no clear response (D. K. Roberts et al. 2016). This was a common refrain with those we spoke to, which was both disconcerting and perplexing as there is no lack of understanding among data security professionals regarding best practices, including the availability of many systems designed to provide high levels of security controls and protection for data/healthcare

data. Vulnerability of data on such devices also puts the manufacturer at risk by exposing protected data to view by unauthorized parties, whereby trust in the security of the system is deeply compromised. These breaches can also result in an event reportable to state or federal entities, depending on the data inappropriately disclosed.

There are also instances of legal violations where data are accessed without authorization by former team employees. In several interviews and at the same SXSW panel, examples were given of employees who stole data when moving jobs from one team to another. Following months of FBI investigations, the scouting director of the St. Louis Cardinals, formerly with the Houston Astros, was recently indicted for twice illegally accessing the Astros' proprietary Ground Control database. He was able to access the club's notes on players, the Astros' draft rankings, scouting reports, and trade notes, as well as a page that listed potential bonus details, statistics and notes on recent performances and injuries by team prospects. In court, the scouting director said he did this in part because he wanted to see if the Astros' new general manager had brought any of the Cardinals' proprietary information with him to Houston (Associated Press 2016a). He confirmed that he indeed had.

Individuals associated with teams relayed that consumers of fantasy sports—a multi-billion dollar industry with over 35 million players worldwide who create imaginary teams of real players of a professional sport based on their performance in actual games—are keenly interested in these data and thus present yet another beneficiary for hackers. Regardless of who the perpetrator or recipient of the unauthorized disclosures, data theft either via hacking or from those within the teams or leagues could lead to public scandal and even players' and others' loss of employment.

Corporate Data Ownership

Another concern about players' personal data is who owns them: the athlete, the team, the league and/or the biometric technology company? In some cases, this is clear: data from games belong

to the NBA, while data collected at practices belong to the teams. But when a technology company contracts with a team to provide biometric data monitoring and analysis, the agreement can be more complex. With some technologies, the teams own these data when they buy the system and the company cannot use team data without permission. Teams may give permission, however, without taking into account or else sidestepping athletes' interests. For teams that own data, if an athlete moves to different a team, the team is at liberty to decide how to handle athlete data: it can be kept privately within a team or sold to or shared with a new team.

Some contracts may state that the technology company owns players' data. The commercial purpose of this provision is to allow the company to use the data for developing and refining its algorithms. Some companies host all the data on their own servers. The implications of this arrangement are manifold. All the previously mentioned data security concerns apply, with transmission of data to the company's servers increasing the risks of hacking or infiltration. Also of concern are both lack of encryption of data at rest and in transit meaning when it is already stored and when it is being transmitted. Again, because the value of the data inheres in its association with individual players, the companies cannot take the usual precaution of anonymizing it. As biometric mobile technologies come into use during games themselves, to monitor players' exertion, etc. in real time, who will have access to these data, either lawfully or unlawfully?

Conflicts of Interest and Dual Loyalty

The availability of greatly expanded personal information on individual players also heightens longstanding concerns about conflicts of interest among people with access to these data. Medical professionals responsible for individuals' physical health and well-being are ethically obligated to place those individuals' interests first. However, medical professionals are far from the only ones with access to health data and they are not the ones gathering, utilizing, and making decisions based on biometric

data. That falls to team trainers and coaches (amongst others) who may not feel or be bound by the same ethical obligations and who have their own and team interests to consider as well. Potential conflicts of interest arise from their relationships within the teams, the authority of coaches and owners, and the pervasive atmosphere of progress, innovation, and data gathering (Testoni et al. 2013), not to mention their own employment and livelihoods. When team coaches and trainers are asked to make crucial decisions based on an athlete's biometric data, it threatens to compromise the trust-based relationships with players that are integral for a player's, and team's, success.

In sport, team physicians, for example, are obligated both to provide care to the individual athlete and to act in the *team's* interest (Testoni et al. 2013) This involves deciding, for example, whether an athlete should return to play, which may not be in an athlete's best interest, but could benefit the team. In the case of professional sports, it may be that "the overwhelming weight of loyalty, and power, is shifted toward the team…: In such circumstances, the physician has both a client and a patient, but it is the client—not the patient—to whom the physician is truly answerable" (King and Robeson 2013).

Often, too, the player at risk wants the same thing as the team (e.g., medical clearance to play in an upcoming game or to continue playing), even if it is not ultimately in the player's best health interest. Players face the internal conflict between what is best for their short-term careers and performance record and for their long-term health. "The athlete's relationship with the team necessarily constrains individual choice…The athlete's role, relationships, and duties with respect to the team constitute an unavoidable framework for individual athlete's decisions" (King and Robeson 2013, 13). This decision calculus may be even more fraught for team trainers and coaches, who ultimately make the calls about players' game-time readiness. With more (albeit unreliable and untested) data, it may be the case that team representatives will be more likely to use the data to extract as much use value from the players as possible with perhaps less regard for players' long-term goals or health.

Andrew Luck, a quarterback for the Indianapolis Colts, said, “The less you have to tell an athletic trainer the better because, you know, it won’t be used against you if you’re trying to get that second, third, or fourth contract…It’s a dilemma” (“Athlete Analytics” 2014). He stressed the importance of trust between players and trainers in making decisions about injuries.

Players’ concerns are largely centered on whether the technologies will be used against them: to say they are not working hard enough, to compare them to others, to keep them from playing, to reduce them to metrics, or to argue they are in a “downward spiral.” Trust will likely to determine how biometric technologies are viewed and whether and which athletes will accept their broader use. The extent of trust between individual players, team personnel, and leagues is complex and influenced by many factors. Some players’ skepticism around the technologies is tied to the long and pervasive history of racial discrimination in the U.S. The racial disparities in some pro sports, such as basketball and football, in which players are predominantly African American and African diasporic, and the front office personnel are predominantly white, will certainly shape the reception of biometric technologies. This discrepancy is equally, if not more, pronounced for positions in the science and conditioning departments where performance directors, sport scientists, and physical therapists oversee the implementation and evaluation of processes that generate such data.

Trust can only be developed when players feel like they are being heard, respected, and treated fairly. With biometric data, some feel that the data are able to speak for themselves, thereby bypassing the need to listen to the “subjective” feelings (of fatigue, readiness, behaviors) of players themselves. As these measures become quantified and objectified, there is a greater risk of using them to the exclusion of players’ own assessments. This could lead to an erosion of trust in the relationships between players and team representatives, lending further suspicion to the intentions of team representatives and the technologies themselves.

The history of racial surveillance that began with transatlantic slavery, as well as racial discrimination in sport and medicine, weave together to provide the context in which these technologies will be viewed. As one team trainer said, "I think a lot of times the players grew up to be skeptical of white people, and rightfully so." Sociologist Simone Browne observes that "surveillance is nothing new to black folks" and notes the "facticity of surveillance in black life" has included slave vessel manifests, plantation inventories, slave patrols, 18th century lantern laws, and contemporary stop-and-frisk policing practices and helicopter monitoring of black neighborhoods (Browne 2015). Black bodies have also long been sites of non-consensual medical and scientific experimentation, and pseudo-medicoscientific theories about Black "inferiority" have been marshalled in the service of white supremacy (Gould 1981; Roberts 2009; Roberts 2012; Reverby 2013; Skloot 2011). One legacy of this violation is that there is often a degree of skepticism of the medical profession and scientific research within the African American community (Tweedy 2015; Hoberman 2012). Sport also long denied Blacks full participation and undoing this legacy has been a slow and arduous process (Carrington 2010; Hawkins 2013; Rhoden 2007). In some sports, lingering feelings of inequity and exploitation manifest as "it's us against you. You are the rich owner and we're the products."

Another potential source of conflict of interest arises when team owners are also investors in the technologies. Dallas Mavericks owner Mark Cuban, for example, is an investor, adviser, and customer of Sport VU, which recently partnered with Catapult. Cuban is "emotionally committed to the business," with the Mavericks being one of Sport VU's early adopters (Burns 2014). With team owners as company investors, the companies' products risk being designed and used with the team owners' rather than the players' interests in mind.

Individual Choice and Coercion

Technologies are never politically neutral; they are always construed within power relationships and their politics are determined by those who mandate or suggest their use. How are players' decisions

to use wearable technologies constrained by the nature of the sport, the organization and politics of a league and its players' unions, or the status of an athlete? Can a player make a free and informed choice about whether or not to use wearable technologies under these conditions, for instance when the league or a team has decided to implement them and when they are purportedly for one's own safety or performance enhancement?

While many of the ethical concerns discussed above could be attended to by stricter regulations and precautions in CBAs and other policies (and hence uniform player contracts), those are unlikely to prevent or curtail the coercive elements of biometric technology use in sport. Coercion can take several forms. Here we focus on those forms that constrain choice—in this case, whether to use biometric technologies as part of one's job. An athlete's degree of autonomy in such matters is dependent on his relationship within and to the team. Power differentials between players and management vary between sports and are in part reflected in the terms of player contracts, the content of which is a mandatory element of collective bargaining. As such, every word and every specific issue that can be subject to an individualized agreement is approved by the players' union.

NBA and MLB players, for example, have contracts that guarantee a player's salary irrespective of performance or injury. The NFL has no such provision: football players are almost never guaranteed compensation, except for signing bonuses, which are paid up front. Management can thus release football players with little financial loss. As a result, "most NFL athletes' contracts create conditions under which the athletes' financial interests almost inevitably come into conflict with their long- and short-term health interests" (Dasgupta and O'Connor 2013). In other words, they may be choosing between job security and serious injury.

Players and teams have a common interest in monitoring to reduce injury risk and promote long-term health and fitness; it is to their joint financial advantage for a player to remain healthy and competitive for as long as possible. But just because a team wants to use the data primarily for injury

prevention does not mean that players should not have the choice whether to use the technology. For some players, the privacy risks may feel too great, but it might be harder to refuse to use them if they are seen as going against their best interests or as the "rookie holdout."

The terms of the contract, such as those in the NFL, can coerce players to acquiesce to invasive uses of technology out of fear of being cut from the team. On some teams, players who do not wear the technology at practice may be fined and excluded from playing. Such policies essentially create a mandate for their use and, in practice, an inability to refuse. One NFL trainer explained that his team is using technologies that include EEGs and ECGs on most players in training and off time. He said: "We just have a culture and a head coach that enforces it. You don't have a choice."

Power differentials in sport occur not just between players and coaches and management, but also among players. Marquee athletes may be able to negotiate the terms of use of these technologies informally or as they do other provisions of their contracts, but those in the lower echelons, competing against one another for playing time or to retain a place on the team, may have little or no leverage. The pressure and desire to maximize playing time is tremendous, leaving many players to adopt or do whatever coaches want that may improve their chances of playing. King and Robeson note "The pressure to perform—or simply to stay healthy (i.e., able to play)—in the setting of a veritable 'arms race' of ever-escalating training, equipment, and facilities profoundly influences an athlete's 'autonomous' decision to accept risks" (King and Robeson 2013). They further argue that, "Athletes should, in at least some circumstances, be regarded as vulnerable to undue, even extreme situational pressures arising from the decision-making environment" (King and Robeson 2013). While previously this put athletes at risk by incentivizing them to "play through the pain," now the incentive may be equally problematic: submitting to invasive and ongoing surveillance.

In all leagues, even where the use of biometric monitoring technology is presented as voluntary, it may have a coercive aspect. Team managers are likely to advocate its role in prolonging athletes'

careers, improving their performance, and protecting them from illness and injury. Those uses are valid and demonstrable, and players may voluntarily agree to monitoring for the same reasons. Yet voluntary use can effectively become coercive if a majority of other players are using the devices and exerting peer pressure, or if players are under tacit pressure to comply because of concerns about keeping a job, renewing a contract, or simply getting playing time. Such concerns are likely to create inequities for the least powerful players on a team.

A snowball effect could ensue. There may come a point in the near future where the 'comparables' (data comparing one individual to others in their class, profession, skillset, etc.) that will be generated from the devices become requisite in hiring decisions, arbitration, and contract negotiations. The imbalanced distribution of knowledge, power, and incentives will always leave athletes in a disadvantaged position. The player may not have all of his own information, and surely will not have comparable information for other players, whereas the team will have both data sets. Players and their unions also may not have sufficient bargaining power to negotiate the protections. Thus, extensive biometric data could increase the bargaining power of teams over players. One possible solution is that players' unions should be given the distribution of outcomes across all players, but this means yet another party has access to these data.

Having more analytics on an athlete can have its tradeoffs. Athletes are commodities whose careers last until they retire or are seriously injured. The increased capacity to assess and even predict injury may affect the career prospects and livelihoods of athletes. Some top draft picks are never offered contracts because of the fear that a prior injury will make them bad investments. One technology analyst observed, "Everyone would like to be able to say a player has this many jumps left on that knee, and maybe somebody's not worth the money because he only has 50 games left in him, but there's no way to know." Even so, based on those who spoke to us, biodata are being used in these types of assessment and contracts are already being affected.

Coercive pressures are not, of course, the only force driving the use of biometric technologies. Many athletes and owners alike are in favor of these technologies and their potential to improve fitness and performance and contribute to career stability and longevity. Matt Hasselbeck of the Indianapolis Colts, for example said "Athletes, we would love to be guinea pigs on something when we're not competing. We'd have no problem trying [them] out" ("Athlete Analytics" 2014). John Brenkus, host of ESPN's *Sport Science* added: "Athletes do love to get information. During the game, you know, they just want to focus on the game. But wanting to know, off the field, how good am I and how can I use that to get better."

AREAS FOR NEGOTIATION AND CONSIDERATION

We see a number of critical areas for immediate deliberation, most especially the development of a sound data governance program, which would include a governing body or council, a defined set of procedures, and a plan to execute those procedures. A board should be designated to develop best practices and to assess and oversee policies and procedures for data collection and management. Ideally, this board would operate from within the players' unions, and even across leagues, to review policies and also the use of particular technologies *prior* to their implementation by a league. It would also be responsible for creating a protocol for data governance.[8]

A board, which could include players, league representatives, medical professionals, sport scientists, and technology representatives, would review: (1) scope of data collection and their use; (2) data ownership and access to data; (3) safeguarding data/baseline security requirements; (4) policy development, oversight, and education. We provide some suggestions for each of these below.

Scope of Data Collection and Use

Threats to privacy are tied to how and when these technologies are used and the kind of data gathered. The tracking of physiological and behavioral characteristics could be said to move beyond privacy concerns to affect a player's rights to freedom of movement and bodily integrity, amongst others. Therefore, leagues must have internal governance controls as to what can be collected, who in the organization can access the data, and for what purposes. It is crucial for teams and players to decide what data can be collected and when and, moreover, what data are sensitive and private and in need of special protective oversight once collected. Further, it seems appropriate to exercise judicious care in implementing these devices: to only use them where they are most effective and appropriate, in order to minimize risks; and data should have a valid, identifiable, and explicit purpose.

Some have called this field "the wild west" with little regard for how technologies are used and to what purpose. Is it truly necessary to generate identifiable data and thus create a record of a player's presence at a certain place and time? Do teams really need chronic, longitudinal data that open the door to ongoing surveillance? This surveillance could reveal personal behavior while also having the ability to locate and track people physically with a high degree of accuracy, placing (particularly, celebrity) players at risk to others who may gain unauthorized access to their location data.

As more knowledge about these devices is generated, incremental implementation that is purposive and focused on particular problems is warranted. This should be considered by teams and players in dialogue with one another, encouraging players' participation. Once decided, there should be methods to ensure that the data collected are limited by their specified purpose and context. How to protect against "scope creep" following software or firmware updates will be an important consideration. This follows the "purpose principle," by which no personal data can be collected without explicit and legitimate purposes and may not exceed the purposes for which they are collected (EU Advisory Body on Data Protection and Privacy 2003). For instance, if sleep monitoring is aimed at tracking insomnia, a team would not then get to use any incidental information collected (that a player

went out late one night, for example) for disciplinary action. This also pertains to setting limits on how long identifiable data are kept.

The boundless nature of the HIAs we saw conflict with these principles. They should be explicit about what information can be collected, the allowable uses of the information as well as what uses are prohibited (for example, personal or commercial), whether data collection is mandatory or voluntary, and the consequences of not complying. It must explicitly lay out a policy regarding third parties. As with other employee contracts, HIAs should be amended for leagues as technologies change and new uses are desired.

Data Ownership and Access to Data

Confidentiality is tied to who owns biometric data as well as who has access to it. Different teams have struck different agreements with vendors regarding ownership, which determines legal rights and also the ability to determine who will be permitted to access it and how they will use it, including the ability to assign, share or surrender all of these privileges to a third party. Teams prefer to own data, but as one team lawyer said, "Ownership is a fluid term." Right now players do not own these data, which is consistent with U.S. privacy law and practices. It is not, however, consistent with EU or Canadian Privacy law. One sports scientist, however, felt players should be able to monetize their data: "They could sell it. There are fantasy fans that want to know all this stuff!" Whether for monetization or not, in our view biometric technology is a human technology "where the ownership and access to one's own body data and other intellectual property must be understood as a right" (Browne 2015, 86).

When determining which personnel should be allowed access, it is imperative that the purpose of access be defined, along with the level and type of access granted (such as view only or updating capability). A second concern is that data for a particular purpose will be retrieved or made available to third parties and used for purposes that the player could neither have predicted nor agreed to. Therefore, leagues need clear policies on data-sharing, including with third parties such as insurance or

law enforcement. In order to protect players, these policies should be as restrictive as possible. Key issues to explore include what happens to data when a contract is terminated with a player or with a vendor? Right now, even if expunging data were required, teams and players have no way of knowing and it may not always be possible to fully expunge these data.

Safeguarding Data/Baseline Security

A third concern is protection of data from alteration, abuse, theft, or unauthorized access or disclosure, any of which could expose the player to harm, discredit, embarrassment, or even extortion. The consequences of a release of personal data can be permanently and irretrievably damaging. Moreover, the slightest publicized breach of confidentiality could easily prevent players' acceptance of these technologies.

Data must be appropriately stored and protected, and their protection monitored. This includes network and application anomaly detection technologies, logging and access control audits, 3rd party penetration tests, intrusion detection and prevention, encryption of data at rest and in transit, and regular vulnerability assessments and risk analyses. Ideally, necessary security measures will be implemented at the beginning of data collection. Data storage and transmission systems must be secured against interception during transmission (and must include encryption of data at rest and in transit), theft of stored data, and intrusion and compromise by those with legitimate access to the data, including athletes, team personnel, and technology companies. The former is especially important because our conversations suggest it is not uncommon for employees to take information and even data with them as they transfer jobs. Companies may promise that they protect privacy, but the end user typically has no way to verify whether such protections are implemented or even effective. Teams should be able to verify any such claims, and to withdraw their data completely if they are not satisfied. Security measures could include encryption, encryption keys, two step sign-ins, multi-factor authentication, and access control logging and auditing to see who has accessed the data. There needs

to be an explicit policy for how long data are retained and subsequently, how they are disposed of. While some types of longitudinal data on a player may be useful, not all data need or ought to be retained indefinitely.

Policy Development, Oversight, and Education

Transparency dictates that clear and commensurate protocols are created and that a culture of accountability is promoted, one which would include penalties for breaches. Given the speed of technology change, the board will need to review new technologies and also new types of biodata being considered for collection, including the changes that accompany software updates which often allow for greater tracking without full disclosures. Educating players will also be critical to developing their trust. At a minimum, answers to the following would be sought: What is the purpose of the technology?; What information is being collected?; How will that information be used and by whom?; How is it being protected?; and, Who will oversee policy development, review, and adherence?

CONCLUSION

The prominence of professional sport in American life is at once a significant driver and rationale for our understanding of the ethics of biometric technologies. These technologies are still in development and their reliability, validity, and interpretability are questionable and uncertain. Despite the fact that we do not yet know how and in which contexts they provide useful data, they have been widely implemented by professional sports leagues. Furthermore, the risks to player privacy, confidentiality, and autonomy are acute in these settings, yet there has been little discussion about these risks or concerted attempts to mitigate them. As leagues enter into collective bargaining negotiations, there will be new opportunities to attend to these issues and we hope our analysis here can contribute to those efforts.

Although professional sport may be in the vanguard for the use of biometric technologies, these

technologies are becoming more widely available and implemented in a variety of settings, including U.S. collegiate and high school sport—which combined enroll millions of people, many children—and other work sectors. The military and commercial flight (e.g., pilots and traffic control) sectors may be the most obvious fields in which to use these next, as they have also already adopted other enhancement technologies in the name of safety and performance (Hoyt and Friedl 2016). We see the potential for expansion of biometric data collection in more pedestrian and wide-reaching settings. Employers are continually looking for ways to maximize employee productivity and reduce costs (from sick days, injuries, "unhealthy" behaviors) and wearable biometric technologies are already being touted as the newest measures to achieve an employer's goals (Silverman 2016). The use of biometric technologies in professional sport is likely to heighten their broad interest and appeal; professional athletes are celebrities and product endorsement (whether official or unofficial) is a facet of their jobs.

The ethical issues we have raised are likely to be of equal concern to the general workforce, perhaps with differing emphases: when biometric technologies are used as tools by bosses, coaches, and others in positions of authority, concerns about privacy, confidentiality, and especially autonomy are omnipresent and urgent. Professional sport can lead the way for others in establishing data governance guidelines, security measures, and the boundaries for employers' and employees' rights and responsibilities for the ethical use of biometric technologies.

Acknowledgements

We owe a huge debt of gratitude to the sport scientists, trainers, coaches, team lawyers, company employees, and players who agreed to speak on the condition of anonymity. We are grateful to Roger Noll, Christine Sublett, Henry Greely, Gary McCoy, Euan Ashley, Leslie Saxon, Jay Porterfield, Brandon Marcello, Lesley Moser, John Protevi, and the anonymous reviewers for their valuable insights. Alexis Garduno provided excellent research assistance.

References

Angwin, Julia. 2016. “Make Algorithms Accountable.” *The New York Times*, August 1. http://www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html?_r=2.

Associated Press. 2016a. “Ex-Cards Exec Pleads Guilty to Hacking Astros.” *ESPN.com*. January 9. http://espn.go.com/mlb/story/_/id/14531169.

———. 2016b. “Report: MLB Approves Players to Wear 2 Devices.” *ESPN.com*. April 5. http://espn.go.com/mlb/story/_/id/15140473.

“Athlete Analytics.” 2014. In *MIT Sloan Sports Analytics Conference*. Cambridge, MA. http://www.sloansportsconference.com/content/athlete-analytics-presented-by-catapult/.

Braun, Lundy. 2014. *Breathing Race into the Machine: The Surprising Career of the Spirometer from Plantation to Genetics*. 1 edition. Minneapolis: Univ Of Minnesota Press.

Browne, Simone. 2015. *Dark Matters: On the Surveillance of Blackness*. Durham: Duke University Press Books.

Burns, Mark J. 2014. “Through Strategic Moves, Catapult Sports Remains Industry Leader In Wearable Technology.” *Forbes*. http://www.forbes.com/sites/markjburns/2014/11/05/through-strategic-moves-catapult-sports-remains-industry-leader-in-wearable-technology/.

Carrington, Ben. 2010. *Race, Sport and Politics: The Sporting Black Diaspora*. London; Thousand Oaks, CA: SAGE Publications Ltd.

Dasgupta, Ishan, and Dan O’Connor. 2013. “From Sports Ethics to Labor Relations.” *The American Journal of Bioethics: AJOB* 13 (10): 17–18. doi:10.1080/15265161.2013.828122.

Department of Justice. 2015. “Overview of The Privacy Act of 1974 (2015 Edition).” https://www.justice.gov/opcl/overview-privacy-act-1974-2015-edition.

Dumit, Joseph. 2004. *Picturing Personhood: Brain Scans and Biomedical Identity*. Princeton: Princeton University Press.

Edmonds, R. C., W. H. Sinclair, and A. S. Leicht. 2013. “Effect of a Training Week on Heart Rate Variability in Elite Youth Rugby League Players.” *International Journal of Sports Medicine* 34 (12): 1087–92. doi:10.1055/s-0033-1333720.

EU Advisory Body on Data Protection and Privacy. 2003. “Working Document on Biometrics: Article 29-Data Protection Working Party.” http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2003/wp80_en.pdf.

“Fitbit Privacy Policy.” 2016. *Fitbit*. https://www.fitbit.com/no/legal/privacy.

Gao, Wei, Sam Emaminejad, Hnin Yin Yin Nyein, Samyuktha Challa, Kevin Chen, Austin Peck, Hossain M. Fahad, et al. 2016. “Fully Integrated Wearable Sensor Arrays for Multiplexed in Situ Perspiration Analysis.” *Nature* 529 (7587): 509–14. doi:10.1038/nature16521.

Gershman, Jacob. 2016. “Prosecutors Say Fitbit Device Exposed Fibbing in Rape Case - Law Blog - WSJ.” April 21. http://blogs.wsj.com/law/2016/04/21/prosecutors-say-fitbit-device-exposed-fibbing-in-rape-case/.

Ghose, Tia. 2015. “New Trackers Claim to Measure Your Stress, But Do They Work?” *Live Science*. January 14. http://www.livescience.com/49452-trackers-measure-stress-heart-rate-variability.html.

Gould, Stephen Jay. 1981. *The Mismeasure of Man*. 1st edition. New York, NY: W. W. Norton.

Greene, Jeremy. 2016. “Do-It-Yourself Medical Devices--Technology and Empowerment in American Health Care.” *New England Journal of Medicine* 374 (4): 305–8.

Hawkins, Billy. 2013. *The New Plantation: Black Athletes, College Sports, and Predominantly White NCAA Institutions*. 2010 edition. New York, NY: Palgrave Macmillan.

Hoberman, J. 2012. *Black and Blue: The Origins and Consequences of Medical Racism*. Berkeley: University of California Press.

Hoyt, Reed, and Karl Friedl. 2016. “The Future of Wearable Tech.” *United States Army Acquisition Support Center*. February 1. http://asc.army.mil/web/the-future-of-wearable-tech/.

Huq, Numaan. 2015. “Follow the Data: Analyzing Breaches by Industry Trend Micro Analysis of Privacy Rights Clearinghouse 2005–2015 Data Breach Records.” https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-follow-the-data.pdf.

Joyce, Kelly Ann. 2008. *Magnetic Appeal: MRI and the Myth of Transparency*. Cornell University Press.

King, Nancy M. P., and Richard Robeson. 2007. “Athlete or Guinea Pig? Sports and Enhancement Research.” *Studies in Ethics, Law, and Technology* 1 (1): 1–17. doi:10.2202/1941-6008.1006.

———. 2013. “Athletes Are Guinea Pigs.” *The American Journal of Bioethics* 13 (10): 13–14. doi:10.1080/15265161.2013.828126.

Korolov, Maria. 2016. “Survey: Health Care Industry Most Targeted by Cyberattackers.” *CSO Online*. April 13. http://www.csoonline.com/article/3055406/data-breach/survey-health-care-industry-most-targeted-by-cyberattackers.html.

Ligaya, Armina. 2014. “High-Tech Sports Pros Seek Edge over Rivals with Wearables.” *Financial Post*, October 23. http://business.financialpost.com/fp-tech-desk/high-tech-sports-pros-seek-edge-over-rivals-with-wearables.

Lowe, Zach. 2015. “From BMI to TMI: The NBA Is Leaning Toward Wearable Tech.” *Grantland*. September 17. http://grantland.com/the-triangle/from-bmi-to-tmi-the-nba-is-leaning-toward-wearable-tech/.

Lupton, Deborah. 2013. “Quantifying the Body: Monitoring and Measuring Health in the Age of mHealth Technologies.” *Critical Public Health* 23 (4): 393–403. doi:10.1080/09581596.2013.794931.

Major League Baseball. 2005. “Addenedum D: Authorization of the Use And/or Disclosure of Major League Player Health Information.” http://mlb.mlb.com/mlb/downloads/joint_drug_prevention_and_treatment_program_2005.pdf.

Malcolm, Dominic. 2016. “Confidentiality in Sports Medicine.” *Clinics in Sports Medicine* 35 (2): 205–15. doi:10.1016/j.csm.2015.10.006.

McCarthy, Jack. 2015. “Healthcare Leads All Industries in Data Breaches.” *Healthcare IT News*. http://www.healthcareitnews.com/news/healthcare-leads-all-industries-data-breaches.

McChrystal, Michael. 2014. “No Hiding the Ball: Medical Privacy and Pro Sports.” *Marquette Sports Law Review* 25 (1): 163–80.

Mehlman, Maxwell J. 2015. “Captain America and ‘Iron Man’: Biological, Genetic and Psychological Enhancement and the Warrior Ethos.” In *Routledge Handbook of Military Ethics*. New York, NY: Routledge.

Mehlman, Maxwell J., and Tracy Yeheng Li. 2014. “Ethical, Legal, Social, and Policy Issues in the Use of Genomic Technology by the U.S. Military.” *Journal of Law and the Biosciences* 1 (3): 244–80. doi:10.1093/jlb/lsu021.

Michael, Katina, and M.G. Michael. 2007. “From Dataveillance to Überveillance and the Realpolitik of the Transparent Society.” https://works.bepress.com/mgmichael/24/.

Morales, J., V. Garcia, X. García-Massó, P. Salvá, R. Escobar, and B. Buscà. 2013. “The Use of Heart Rate Variability in Assessing Precompetitive Stress in High-Standard Judo Athletes.” *International Journal of Sports Medicine* 34 (2): 144–51. doi:10.1055/s-0032-1323719.

Nakamura, Fabio Y., Lucas A. Pereira, Felipe N. Rabelo, Andrew A. Flatt, Michael R. Esco, Maurizio Bertollo, and Irineu Loturco. 2016. “Monitoring Weekly Heart Rate Variability in Futsal Players during the Preseason: The Importance of Maintaining High Vagal Activity.” *Journal of Sports Sciences*, May, 1–7. doi:10.1080/02640414.2016.1186282.

NBA D-League. 2015. “NBA D-League National Tryouts Player Release & Eligiblity Form.” NBA D-League. https://dleaguetryouts.nba.com/2015_NBA_D-League_National_Tryout_Waivers-Release_Eligibility_and_Consent_Authorization.pdf.

NFL. 2011. “Collective Bargaining Agreement.” *NFL Laborfiles*. August 4. https://nfllabor.files.wordpress.com/2010/01/collective-bargaining-agreement-2011-2020.pdf.

OECD. 1980. “OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.” https://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

Pappas, Stephanie. 2014. “Will Wearable Tech Bring Humanity a ‘Sixth Sense?’” *LiveScience.com*. January 10. http://www.livescience.com/42490-wearable-biosensor-technology.html.

Perez, A.J. 2016. “MLB, Apple Strike Agreement: iPads in Dugouts.” *USA TODAY*. March 30. http://www.usatoday.com/story/sports/mlb/2016/03/30/mlb-apple-strike-agreement-ipads-dugouts/82417430/.

Ponemon Institute. 2016. “Sixth Annual Ponemon Benchmark Study on Privacy & Security of Healthcare Data Incidents | ID Experts.” Ponemon Institute. https://www2.idexpertscorp.com/sixth-annual-ponemon-benchmark-study-on-privacy-security-of-healthcare-data-incidents?utm_source=Referral&utm_medium=press%20release&utm_campaign=Ponemon%202016.

Rapp, Rayna. 1999. *Testing Women, Testing the Fetus: The Social Impact of Amniocentesis in America*. New York: Routledge.

Reverby, Susan M. 2013. *Examining Tuskegee: The Infamous Syphilis Study and Its Legacy*. Reprint edition. Chapel Hill: The University of North Carolina Press.

Rhoden, William C. 2007. *Forty Million Dollar Slaves: The Rise, Fall, and Redemption of the Black Athlete*. Reprint edition. New York: Broadway Books.

Roberts, Daron K., Brandon E. James, Emmanuel Acho, and Roderick Moore. 2016. “1984 Meets Moneyball: Who Owns Player Data?” In *SXSW*. Austin, TX.

Roberts, Dorothy. 2009. “Margaret Sanger and the Racial Origins of the Birth Control Movement.” In *Racially Writing the Republic: Racists, Race Rebels, and Transformations of American Identity*, edited by Bruce Baum and Duchess Harris. Durham, NC: Duke University Press.

———. 2012. *Fatal Invention: How Science, Politics, and Big Business Re-Create Race in the Twenty-First Century*. New York: The New Press.

Schüll, Natasha Dow. 2016. “Data for Life: Wearable Technology and the Design of Self-Care.” *BioSocieties*, March. doi:10.1057/biosoc.2015.47.

Siebert, Dave. 2014. “An Inside Look into the NFL Medical Exam Process at the Combine.” *Bleacher Report*. http://bleacherreport.com/articles/1968230-an-inside-look-into-the-nfl-medical-exam-process-at-the-combine.

Silverman, Rachel Emma. 2016. “Bosses Tap Outside Firms to Predict Which Workers Might Get Sick.” *Wall Street Journal*, February 18, sec. Business. http://www.wsj.com/articles/bosses-harness-big-data-to-predict-which-workers-might-get-sick-1455664940?cb=logged0.5834580201189965.

Skloot, Rebecca. 2011. *The Immortal Life of Henrietta Lacks*. New York: Broadway Books.

Stotts, Jeff. 2014. “NBA Injury Analysis.” *In Street Clothes*. http://instreetclothes.com/nba-injury-analysis/.

Swetlitz, Ike. 2016. “Sweat-Sensing Bracelet Could Be next Wearable Tech.” *STAT*. January 27. http://www.statnews.com/2016/01/27/sweat-wearable-tech/.

Talukder, Hisham, Thomas Vincent, Geoff Foster, Camden Hu, Juan Huerta, Aparna Kumar, Mark Malazarte, Diego Saldana, and Shawn Simpson. 2016. “Preventing in-Game Injuries for NBA Players.” In . Boston, MA. http://www.sloansportsconference.com/wp-content/uploads/2016/02/1590-Preventing-in-game-injuries-for-NBA-players.pdf.

Tenney, Dave. 2015. Interview.
Testoni, Daniela, Christoph P. Hornik, P. Brian Smith, Daniel K. Benjamin, and Ross E. McKinney. 2013. "Sports Medicine and Ethics." *The American Journal of Bioethics: AJOB* 13 (10): 4–12. doi:10.1080/15265161.2013.828114.
Timmermans, Stefan. 2010. *Sudden Death and the Myth of CPR*. Temple University Press.
Torre, Pablo S., and Tom Haberstroh. 2014. "Advanced, Increasingly Invasive Tests Being Used to Monitor NBA Players." *ESPN.com*. October 10. http://espn.go.com/nba/story/_/id/11629773.
Tweedy, Damon. 2015. *Black Man in a White Coat: A Doctor's Reflections on Race and Medicine*. 1 edition. New York: Picador.
U.S. Department of Health and Human Services. 2002. *Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53,182, 53,193 (Aug. 14, 2002) (to Be Codified at 45 C.F.R. Pt. 160 & 164)*. http://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/privacyrule/privruletxt.txt.
———. 2016. "Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA." U.S. Department of Health and Human Services. https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.
Westover, Boden. 2016. "Website Enquiry," June 1.
"WHOOP." 2016. Accessed June 3. http://whoop.com/.

[1] Estimates the financial loss due to injury is exceedingly complex. These calculations, which were derived by multiplying the number of games lost to injury by the player's salary per game, are illustrative of potential losses due to injury, but they are far from comprehensive enough to be taken at face value.

[2] Although these technologies are also in use by women's teams and individual women athletes internationally, their use in the U.S. is more prevalent in the heavily financed world of men's professional sport. We imagine they will become more widely adopted by women's teams in the near future and will raise concerns specific to women athletes, the most obvious of which is the ability for such technologies to detect pregnancy.

[3] The privacy policy indicates all data are stored on servers in the European Union. Under the section "How Do We Keep Your Data Safe," there is very little in the way of specific controls, including whether the data are encrypted at rest, which means data in persistent storage.

[4] The U.S. Privacy Act of 1974 has embedded in it a code of fair information practices, which provide a privacy framework and safeguard requirements for automated personal data, but it directly applies to federal executive branch agencies. Moreover, the Act's "imprecise language, limited legislative history, and somewhat outdated regulatory guidelines" make it difficult to interpret and apply (Department of Justice 2015). The Organization for Economic Co-operation and Development (OECD), an international

forum for countries to work together to solve global problems, adopted privacy guidelines in the 1980s with the goals of integrating data security across the spectrum of government and business usage of personal data, as well as online usage of such data (OECD 1980). The OECD principles are closely tied with the European Union legislation as contained in the Data Protection Directive 95/46/EC where "personal data" is framed broadly as "any information relating to an identified or identifiable individual." In 2013 the European Commission announced new data protection regulations to address how mobile apps should comply with EU data protection law, which is part of the EU privacy and human rights law.

[5] For a good discussion see Andrew Flatt: https://www.freelapusa.com/interpreting-hrv-trends-in-athletes-high-isnt-always-good-and-low-isnt-always-bad/

[6] This is a particular risk during software or firmware updates—a player would likely not know that the scope of collection had changed.

[7] The NBA CBA, Section 3: Disclosure of Medical or Health Information, states:

(a) A Team physician may disclose all relevant medical information concerning a player to (i) the General Manager, coaches, and trainers of the Team by which such player is employed, (ii) any entity from which any such Team seeks to procure, or has procured, an insurance policy covering such player's life or any disability, injury or illness such player may suffer or sustain, and (iii) subject to the terms of Section 3(d) below, the media or public on behalf of the Team

Sections 3(d) and (e) of the NBA CBA reads as follows:

(d) Subject to Section 3(e) below, each Team may make public medical information relating to the players in its employ, provided that such information relates solely to the reasons why any such player has not been or is not rendering services as a player.

(e) A player or his immediate family (where appropriate) shall have the right to approve the terms and timing of any public release of medical information relating to any injuries or illnesses suffered by that player that are potentially life- or career-threatening, or that do not arise from the player's participation in NBA games or practices.

[8] Microsoft has developed a Data Governance for Privacy, Confidentiality and Regulatory Compliance (DGPC) framework that may serve as a model.